REMARKS

Claims 1-56 are pending in the present application. Claims 1, 4, 11, 16, 17, 19, 22, 34, 35, 38, 41, 46-48 and 54 have been amended herewith. Reconsideration of the claims is respectfully requested.

I. Claim Objection

The Examiner objected to Claims 1-56, stating that a definition for inline crypto engine has not been provided. This objection is traversed as follows.

Applicants have amended Claims 1, 19 and 38 to define the inline crypto engine. Thus, the objection to Claim 1-56 has been overcome.

II. 35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 1-56 under 35 U.S.C. § 103(a) as being unpatentable over Jardin (U.S. Patent No. 6,681,327) (hereinafter "Jardin") in view of Matsumoto et al. (*Speeding Up Secret Computations with Insecure Auxiliary Decides"*, 1990*)* (hereinafter "Matsumoto"). This rejection is respectfully traversed.

Applicants initially traverse the rejection of Claim 1 by showing that the references have been improperly combined using hindsight analysis. The Examiner states that the cited Jardin reference does not teach the claimed inline crypto engine, but states that the cited Matsumoto reference teaches a server that performs the function of secret computation, encryption and decryption, on behalf of a client device. The Examiner then states it would have been obvious to add the trustworthy server and delegate the encryption and decryption calculations to a separate server as in Matsumoto in the broker and server system of Jardin, the motivation for combining these teachings being that the system is a trusted network wherein the computing power of the auxiliary device may be implemented. Applicants urge that since Jardin teaches that his broker decrypts packets received from a client (Figure 3, blocks 330 and 340), and his transaction server encrypts certain response packets sent to the client (Figure 4, block 436), there would have been no reason or other motivation to include an additional device such as Matsumoto's server for encryption and decryption to the teachings of Jardin, *as Jardin already possesses processing blocks and associated functionality to perform* *encryption and decryption*. The only motivation for combining the teachings of Matsumoto with the teachings of Jardin must therefore be coming from Applicants' own patent specification, which is improper hindsight analysis. It is error to reconstruct the patentee's claimed invention from the prior art by using the patentee's claims as a "blueprint". When prior art references require selective combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight obtained from the invention itself. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 227 USPQ 543 (Fed. Cir. 1985). Because there would have been no motivation to combine Matsumoto's encryption/decryption server with Jardin's system, which already fully provides encryption and decryption functionality, the only reason for the combination must be coming from the hindsight obtained from the present invention itself, which is improper hindsight analysis.

Applicants further show that there would have been no motivation to include the teachings of Matsumoto with the teachings of Jardin, as the encryption/decryption provided by Matsumoto's server is not secure or trustworthy (see, e.g., Matsumoto's Title of "Speeding Up Secret Computations with *Insecure* Auxiliary Devices" (emphasis added by Applicants); see also Matsumoto Abstract on page 497; see also Matsumoto page 498, paragraphs 1 and 2). As stated by the Examiner in the motivation to combine the references, "the system is a trusted network wherein the computing power of the auxiliary device may be implemented". Because Matsumoto's system is not trusted, a person of ordinary skill in the art would not have been motivated to include such an untrusted component into a trusted system as taught by Jardin. This further evidences no motivation to combine these two cited references, as the trustworthiness of Jardin's system would be compromised. Thus further evidences that the references have been improperly combined, as a person of ordinary skill in the art would not have been motivated to combine such references as described above.

Even when the references have been improperly combined, Applicants show that there is still at least one missing claimed feature not taught or suggested by the cited references, further evidencing non-obviousness. In particular, none of the ~~cited~~ references teach or suggest utilizing one engine (an online crypto engine) to perform encryption or decryption *using cryptographic parameters established by another engine* (a handshake engine). In rejecting this aspect of Claim 1, the Examiner cites Matsumoto's server as teaching the claimed inline crypto engine, and Jardin's broker 120 as teaching the claimed handshake engine. Because these two devices (Matsumoto's server and Jardin's broker) are described in two separate references, it necessarily follows that there is no teaching or suggestion of the claimed co-action between such devices (as they are both described separately in their respective individual teachings), and in particular there is no teaching or suggesting of using parameters establish by one of these devices (Jardin's broker) by the other of these devices (Matsumoto's server). Thus, even when the references have been improperly combined, there is still at least one missing claimed element, further evidencing non-obviousness. To establish prima facie obviousness of a claimed invention, <u>all</u> of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03 (emphasis add by Applicants); *see also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). In the absence of a proper *prima facie* case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent. *See In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). The claimed co-action between the handshake engine and the inline crypto engine advantageously provides an ability to separate the handshaking functionality from the encryption/decryption functionality to improve performance, as the handshaking functionality is inherently much slower to perform (Specification page 13, lines 13-20). Per the present invention, this handshake functionality can be performed by a separate handshake engine, thus offloading the handshake operations that would otherwise hinder the performance of the encryption/decryption engine (Specification page 14, lines 20-22).

Still further with respect to Claim 1, because of Jardin's desire to use a common broker to provide *both* (i) handshake and decryption for a client (column 4, line 35 – column 6, line 3), *and* (ii) handshake and encryption for a back-end transaction server (column 7, lines 6-19), there would be no motivation to somehow separate the handshake and encryption/decryption functionality and still provide such dual-purpose functionality by a common broker, as expressly desired by the teachings of the cited Jardin reference – further evidencing no motivation to modify the teachings of Jardin in accordance with the claimed invention.

Applicants initially traverse the rejection of Claims 2-18 and 48 for reasons given above regarding Claim 1 (of which Claims 2-18 and 48 depend upon).

Further with respect to Claim 4, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the establishing step includes handing off a network connection from the transaction server to the handshake engine". In rejecting Claim 4, the Examiner cites Jardin's Figure 3 as teaching this claimed feature. Applicants urge that Jardin's Figure 3 describes the internal process flow between a broker 120 and a transaction server 130 (Jardin column 6, line 4 – column 7, line 56). Notably, it is Jardin's broker (which allegedly reads on the claimed handshake engine) that hands-off the communication link to a transaction server (Jardin, column 6, lines 39-41), which is just the opposite of what is recited in Claim 4, where the network connection is handed-off *from* the transaction server *to* the handshake engine. In any event, Applicants have amended Claim 4 to further clarify and distinguish the invention recited therein from the teachings of the cited references. Thus, Claim 4 is further shown to not be obvious in view of the cited references.

With respect to Claims 16 and 17, Applicants have amended such claims to specify that the inline crypto engine receives/transmits data from/to the network. In other words, the claimed inline crypto engine is located at the front-end of the system. In contrast, Matsumoto's server (which is alleged to read on the claimed inline crypto engine) is a back-end processor. Thus, Claims 16 and 17 are further shown to not be obvious in view of the cited references.

With respect to Claim 19 (and dependent Claims 20-37) and Claim 38 (and dependent Claims 39-47 and 49-56), Applicants traverse for similar reasons to those given above with respect to Claim 1.

Further with respect to Claims 22 and 41, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 4.

Further with respect to Claims 34 and 35, Applicants traverse for similar reasons to the further reasons given above with respect to Claims 16 and 17.

Further with respect to Claim 52, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the at least one transaction server receives a request to establish the cryptographic parameters; and responsive to the at least one transaction server's receiving the request, the at least one handshake engine performs the establishing step". In rejecting Claim 52, the Examiner alleges that Jardin teaches the features of Claim 52 at Jardin's Figure 2. Applicants urge that Jardin's Figure 2 is with respect to communication between a client 110 and a broker 120, and provides no teaching/suggestion of any transaction server, and in particular provides no teaching/suggestion of a transaction server that receives a request to establish the cryptographic parameters, as expressly recited in Claim 52. Thus, Claim 52 is further shown to not be obvious in view of the cited references.

Therefore, the rejection of Claims 1-56 under 35 U.S.C. § 103 has been overcome.

III. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 3/2/05

Respectfully submitted,

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicant